



ACTA DE SORTEO CERTIFICADO

SORTIVEN V1.4 — Sistema de Sorteo Auditable · Aleatoriedad Verificable (Provably Fair)

1. Identificación del Sorteo

ID del sorteo	4621c3a4-e04f-486b-a557-a952784b801f
Nombre	[DEMO SENCAMER] Falcón Animalitos – Ruleta Virtual — muestra 005
Tipo de juego	Animalitos
Estado	revelado
Versión del algoritmo	rng-v1
Creado	2026-08-25T05:38:04Z
Ejecutado	2026-08-25T05:38:04Z
Revelado	2026-08-25T05:38:04Z

2. Resultado Oficial

12 · Caballo

3. Evidencia Provably-Fair

Compromiso (SHA-256) — pre-sorteo	7f9b60bef6e6236c1febce5989e65e09878dc4048b33091c0421b45aa55f2bab2
Semilla del cliente (client seed)	sencamer-demo-animalitos-005
Nonce	5
Semilla del servidor (revelada)	dc8d67b08cf8566f9d577ccbaacd12fd20117fa58e2db719a84a55b36a1a20ae

4. Cadena de Auditoría (Ledger inmutable)

Índice en la cadena	36
Hash anterior (prev_hash)	15f1e539fc8e5c6740aec93d1b719450a225443c6d1d2341c8e5992ec3eacf4
Hash del registro (record_hash)	52aa5de2c32ca7863129f3b17d29be6aa5dd8bee019fa6f273bde08b17e3339d

5. Cómo Verificar este Sorteo

Cualquier persona puede verificar la integridad de este sorteo: (1) Confirme que SHA-256 de la **semilla del servidor revelada** es igual al **compromiso** publicado antes del sorteo. (2) Recompute el resultado con (semilla servidor, semilla cliente, nonce) usando el algoritmo público **HMAC-SHA256** con muestreo por rechazo. (3) Verifique el **record_hash** recalculando SHA-256(prev_hash + datos canónicos). El portal público de verificación realiza estos pasos automáticamente.